



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,776	11/15/2001	Esa Turtiainen	032986-019	4500
27045	7590	06/21/2006	EXAMINER GELAGAY, SHEWAYE	
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR C11 PLANO, TX 75024			ART UNIT 2137	PAPER NUMBER

DATE MAILED: 06/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/003,776	Applicant(s) TURTIAINEN ET AL.	
	Examiner Shewaye Gelagay	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on May 22, 2006. Claims 1 and 5 have been amended. Claims 1-7 are pending.

Specification

2. In view of the amendment filed May 22, 2006, the Examiner withdraws the objection to the specification.

Claim Rejections - 35 USC § 112

3. In view of the amendment filed May 22, 2006, the Examiner withdraws the rejection of claims 1-7 under 35 U.S.C. 112.

Response to Arguments

4. Applicant's arguments filed May 22, 2006 have been fully considered but they are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

Applicant's arguments regarding Mamros or Patel do not teach, "using a first security association to establish a second security association, which is then modified by selected components of the second protocol". The applicant has argued this limitation is supported in paragraphs 36-38 of the disclosure submitted. According to the disclosure IKE phase 1 negotiation is used to share a secret or "key" between the peers and entering IKE phase 2 to negotiate a pair of SAs. Modifying is taught as the IPsec

SA data relevant to encryption including a pair of encryption, is then passed to the VOIP applications. Patel teaches ISAKMP/OAKLEY key management protocol defined by IPsec for authentication, security association and key management. The protocol defines two phases, phase 1 the peers are authenticated, the security association and keying material is agreed. Phase 2 is used to negotiate security association for security applications (e.g. IPSEC AH and ESP). Patel further discloses the keying material from the phase 1 is used to generate session keys for the secure communication applications. Phase 2 can be used subsequently for key refresh on per need bases in the future. (Page 1, paragraph 5; page 2, paragraph 1) Therefore, Patel teaches using the first security association to establish a second security association, which is then modified by selected component of the second protocol.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269

in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel).

As per claims 1 and 5:

Mamros teach a method of sending streamed data over an IP network from a first node to a second node, the method comprising:

using a first protocol to establish a first security association (SA1) between the first and second nodes; (Col. 6, lines 9-13)

constructing datagrams containing segments of the encrypted streamed data in the datagram payload, the datagrams including a reduced overhead corresponding to the selected components; (Col. 5, lines 51-67 and Col. 6, lines 1-7) and

sending the datagrams from the first node to the second node. (Col. 2, lines 44-45; Col. 3, lines 15-30 and lines 45-47)

In addition, Mamros discloses sending encrypted streamed data and establishing secure and authenticated channel using ISAKMP/Oakley protocol. (Col. 6, lines 2-22)

Mamros does not explicitly disclose using a first protocol to establish a first security association (SA1) over a second protocol between the first nodes and second nodes; and modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first and second node.

Patel in analogous art, however, discloses using a first protocol to establish a first security association (SA1) over a second protocol between the first nodes and second nodes; (Page 1, paragraph 5; page 2, paragraph 1; *phase 1 negotiation is interpreted as*

Art Unit: 2137

the first protocol and phase 2 negotiations is interpreted as the second protocol, the interpretation is given based on description given in the specification, page 6, paragraphs 2 and 3) and modifying the second security association (SA2) by using selected components of the second protocol for providing encryption at the first node of the streamed data between the first and second node; (Page 1, paragraph 5; page 2, paragraph 1) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Mamros with Patel in order to reduce a startup time for communication and improve the efficiency of the protocol. Patel (Page 2, paragraph 2; Patel)

As per claim 3:

The combination of Mamros and Patel teaches all the subject matter as discussed above. In addition, Mamros further discloses a method wherein said first and second nodes are end points for the data. (Figure 1; Col. 3, lines 27-29)

As per claim 4:

The combination of Mamros and Patel teaches all the subject matter as discussed above. In addition, Mamros further discloses a method wherein said first and second nodes tunnel data between respective end points. (Figure 2; Col. 3, lines 27-29)

As per claim 6:

The combination of Mamros and Patel teaches all the subject matter as discussed above. In addition, Mamros further discloses an apparatus, the apparatus being an end user terminal such as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC). (Figure 2; Col. 3, line 15)

Art Unit: 2137

7. Claims 2 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mamros et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269 in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter Patel) further in view of Dutnall United States Letter Patent Number 6,584,098.

As per claim 2:

The combination of Mamros and Patel teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.

Dutnall in analogous art, however, discloses a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. (Col. 13, lines 22-28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros and Patel to include a method wherein said streamed data is VoIP data or videoconferencing data, wherein said streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. This modification would have been obvious because a person having ordinary skill in the art would have

Art Unit: 2137

been motivated to do so, as suggested by, Dutnall (Col. 3, lines 51-52) in order to avoid excessive delay to a voice signal by reducing significant extra processing overhead.

As per claim 7:

The combination of Mamros and Patel teaches all the subject matter as discussed above. In addition, Mamros further discloses an apparatus, the apparatus being a firewall or gateway coupled to the first node which is the source of the streamed data. (Figure 2; Col. 3, line 23)

Both references do not explicitly disclose a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers.

Dutnall in analogous art, however, discloses a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. (Col. 13, lines 22-28)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros and Patel to include a method wherein the streamed data packets do not include IPSec headers, authentication headers (AH) and encapsulation security payload (ESP) headers. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Duntall (Col. 3, lines 51-52) in order to avoid excessive delay to a voice signal by reducing significant extra processing overhead.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER